Comprendere la categoria Sicurezza potenzialmente dannosa in Umbrella

Sommario

Introduzione

Questo documento descrive la categoria di sicurezza Potenzialmente dannosa di Cisco Umbrella.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

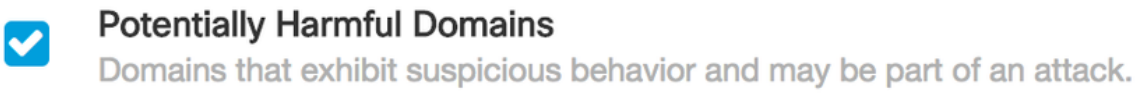
Componenti usati

Le informazioni fornite in questo documento si basano su Cisco Umbrella.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica

I clienti Umbrella hanno livelli diversi di tolleranza al rischio quando si tratta di sicurezza. A seconda del settore e del tipo di lavoro svolto, può essere utile monitorare e bloccare in modo proattivo le attività potenzialmente dannose. La nuova impostazione di protezione "Potenzialmente dannosa" è disponibile in Prevenzione accanto ad altre impostazioni di protezione ed è impostata su Consenti per impostazione predefinita:



115011476788

Dettagli

Potenzialmente dannoso è una categoria di sicurezza che contiene domini che potrebbero essere dannosi. È diverso dalle categorie "malware" di Umbrella perché Umbrella li classificava con un livello di confidenza più basso sul fatto che fossero effettivamente dannosi. Secondo i nostri analisti e gli algoritmi che usiamo per determinare in generale, ma non necessariamente per essere dannosi, questi domini sono considerati sospetti.

L'utilizzo di questa categoria dipende dalla tolleranza dimostrata nei confronti del rischio di bloccare i domini potenzialmente validi. Se si dispone di un ambiente altamente sicuro, questa è una buona categoria da bloccare e se l'ambiente è più libero, è sufficiente consentire e monitorare.

Se non sei sicuro di quali tra questi aspetti ti trovi, puoi monitorare le attività che nelle tue segnalazioni sono state indicate come "Potenzialmente dannose". La disponibilità di questa categoria può fornire una maggiore granularità nella classificazione del traffico, aumentare la visibilità, fornire una maggiore protezione e migliorare la risposta ai problemi. Ad esempio, se si ritiene che una macchina sia infetta da malware, se si considerano i domini potenzialmente dannosi visitati, è possibile valutare meglio il livello di compromissione.

Umbrella determina ciò che è "Potenzialmente dannoso" pesando diversi fattori che indicano che, sebbene il dominio non sia chiaramente dannoso, potrebbe rappresentare una minaccia. Esistono, ad esempio, diversi tipi di servizi di tunneling DNS. Alcuni di questi servizi rientrano nelle categorie dei VPN benigni, dannosi e di tunneling DNS, ma alcuni sono più poco chiari e non rientrano in nessuna di queste categorie. Se lo scenario di tunneling è sconosciuto e sospetto, la destinazione può essere classificata nella categoria Potenzialmente dannoso.

Un altro esempio viene dal modello del rango Spike di Umbrella. Il modello di classificazione dei picchi di Umbrella sfrutta enormi quantità di dati di richiesta DNS e rileva i domini che hanno picchi nei loro modelli di richiesta DNS utilizzando la grafica delle onde sonore. Il traffico che raggiunge livelli elevati nel dominio di classificazione Spike può essere classificato automaticamente come dannoso e il traffico più basso nella soglia può rientrare nella categoria Potenzialmente dannoso.

Per segnalare i rilevamenti indesiderati in una di queste categorie:

- Inviare tutte le richieste di classificazione dei dati a Cisco Talos tramite il supporto Talos.
- Per la procedura generale di invio delle richieste a Cisco Talos, vedere Procedura: Inviare Una Richiesta Di Categorizzazione.

Per la categoria Potenzialmente dannoso, Umbrella non la riclassifica come sicuro senza avere la

garanzia che il dominio è assolutamente legittimo.

Nei report è possibile filtrare entrambe le categorie come qualsiasi altra categoria di protezione.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).